PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

REG'D 2 1 AUG 2003

The Patent Office
Concept House
Cardiff Road
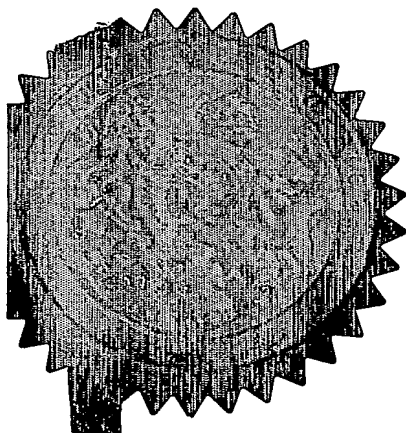Newport
South Wales
NP10 8QQ
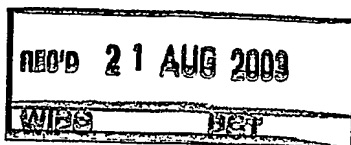
I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4)
of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the
Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as
originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named
in this certificate and any accompanying documents has re-registered under the Companies Act
1980 with the same name as that with which it was registered immediately before re-
registration save for the substitution as, or inclusion as, the last part of the name of the words
"public limited company" or their equivalents in Welsh, references to the name of the company
in this certificate and any accompanying documents shall be treated as references to the name
with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c.,
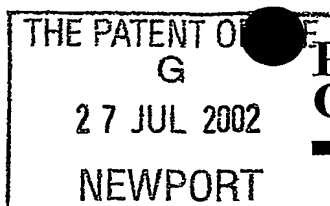plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely
subjects the company to certain additional company law rules.

Signed

Dated   2 May 2003

Form 1/77

tents Act 1977
le 16)

THE PATENT OFFICE
G
2 7 JUL 2002
NEWPORT

The
Patent
Office

1/77

:quest for grant of a patent
:e notes on the back of this form. You can
o get an explanatory leaflet from the Patent
fice to help you fill in this form)

The Patent Office
Cardiff Road
Newport
Gwent NP10 8QQ

Your reference	PHGB 020118

29 JUL 02 E736818-1 002879
P01/7730 0.00 0217462.1

Patent application number *(The Patent Office will fill in this part)*	0217462.1	2 7 JUL 2002

Full name, address and postcode of the or of each applicant *(underline all surnames)*	KONINKLIJKE PHILIPS ELECTRONICS N.V. GROENEWOUDSEWEG 1 5621 BA EINDHOVEN THE NETHERLANDS
Patents ADP Number *(if you know it)*	7419 294001
If the applicant is a corporate body, give the country/state of its incorporation	THE NETHERLANDS

itle of the invention	STORAGE OF ENCRYPTED DIGITAL SIGNALS

Name of your agent *(if you have one)* "Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*	ANDREW GORDON WHITE Philips Intellectual Property and Standards Cross Oak Lane Redhill Surrey RH1 5HA
Patents ADP number *(if you know it)*	7133 473003

If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number	Country	Priority Application number *(if you know it)*	Date of filing *(day/month/year)*

If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application	Number of earlier application	Date of filing *(day/month/year)*

Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer "Yes" if:* a) *any applicant named in part 3 is not an inventor, or* b) *there is an inventor who is not named as an applicant, or* c) *any named applicant is a corporate body.*	YES

Patents Form 1/77

Patents Form 1/77

9. Enter the number of sheets for any of the following
   items you are filing with this form.
   Do not count copies of the same document.

Continuation sheets of this form		
Description	7	
Claims(s)	3	
Abstract	1	
Drawings	3	only

10. If you are also filing any of the following,
   state how many against each item:

   Priority Documents

   Translations of priority documents

   Statement of inventorship and right

   to grant of a patent (*Patents Form 7/77*)

   Request for preliminary examination and

   search (*Patents Form 9/77*)

   Request for substantive examination

   (*Patents Form 10/77*)

   Any other documents

   (*Please specify*)

11. I/We request the grant of a patent on the basis of this application.

   Signature _____ Date 26/7/2002

12. Name and daytime telephone number of
   person to contact in the United Kingdom   01293 815438   (A. G. WHITE)

Patents Form 1/77

DESCRIPTION

STORAGE OF ENCRYPTED DIGITAL SIGNALS

5

The present invention relates to the storage of digital signals, particularly but not exclusively to decrypting received digital video signals using a broadcaster's encryption system, manipulating the decrypted signals to improve recording/playback operation and re-encrypting the signals using the

10   same encryption system.

When digital video signals are recorded, for example on a hard disk or optical disk, copy protection of the content is often required. The usual method of achieving this is to encrypt the signals prior to transmission using a

15   cryptographic algorithm, also known as a cipher. The signals are fed into the cipher together with data known as a key, to generate an encrypted signal. Decryption is achieved by using the same algorithm and the same key to recover the original unencrypted signals. Normally, the cipher function does not change, but the keys change frequently. This type of key-based algorithm

20   is generally known as a symmetric or secret-key algorithm.

Many digital television channels are encrypted for transmission, either to restrict access to only those consumers who have paid for the channels, or to limit the broadcast to a particular geographical region.

A known method of ensuring copy protection in recording such

25   encrypted channels is to record the signal from the broadcast as is, without decoding the decryption used for the transmission.

Another known method is to encrypt the broadcast stream a second time before storage.

The storage of data in accordance with these methods is attractive for

30   the broadcaster, since it maintains conditional access rights on the stored content and the content is encrypted with a technology trusted by the broadcaster. However, this solution is unattractive for the video storage device

manufacturer, because it means that the storage device must store the signal in exactly the format it was received. This removes the ability to perform manipulations on the data to make the signal easier to record or to play back.

One method which removes this constraint is to decrypt the broadcast,
5   process it and then re-encrypt it with a different cipher function and different set of keys. However, this method breaks the link with the broadcaster's encryption system and is therefore undesirable from the broadcaster's perspective.

10   The present invention aims to address the above problems.

According to the invention there is provided a method of storing a received digital signal which has been encrypted by an encryption key and transmitted in encrypted form, comprising the steps of decrypting the signal using a decryption key corresponding to the encryption key, processing the
15   decrypted signal, re-encrypting the processed signal using the encryption key and storing the re-encrypted signal.

The processing may comprise operations which manipulate the signal to improve storage and/or playback operation, such as PID remapping, remultiplexing and/or transcoding.
20   By processing the signal in decrypted form and re-encrypting it using the same encryption system as was used for transmission by, for example, a broadcaster, manipulation of the signal to improve recording and/or playback is permitted, while maintaining the integrity of the broadcaster's encryption system.
25   According to the invention there is further provided a digital signal storage device for storing a digital signal which has been encrypted using an encryption key and transmitted in encrypted form, the device comprising decryption means for decrypting the signal using a decryption key corresponding to the encryption key, means for processing the decrypted
30   signal, encryption means for re-encrypting the processed signal using the encryption key and means for storing the re-encrypted signal.

The decryption key may be the same as the encryption key and each of these keys may be one of a plurality of keys forming a key stream. The key stream may be delayed prior to re-encrypting the decrypted signal and the delay may be dependent on the processing being carried out.

5   According to the invention there is still further provided digital signal recording apparatus for recording a digital signal which has been encrypted using an encryption key and transmitted in encrypted form, the apparatus comprising a decryption module for decrypting the signal using a decryption key corresponding to the encryption key, a processor for processing the

10   decrypted signal, an encryption module for re-encrypting the processed signal using the encryption key and a storage medium for storing the re-encrypted signal.

Embodiments of the invention will now be described, by way of

15   example, with reference to the accompanying drawings, in which:

Figure 1 is a schematic diagram of a conventional digital television broadcasting system;

Figure 2 is a schematic diagram illustrating a recording device according to the invention;

20   Figure 3 is a flow diagram illustrating the operation of the recording device of Figure 2; and

Figure 4 is a schematic diagram illustrating a variation on the recording device of Figure 2.

25   Referring to Figure 1, in a conventional digital television broadcasting system, content to be broadcast, including for example, video, audio and data components, is encoded in an encoder 1 using an appropriate coding system, for example MPEG-II for digital broadcasting, in which a digital signal is represented as a stream of transport packets. The encoded broadcast stream

30   is encrypted in a first encryption module 2 using a cryptographic key referred to as a control word CW, which is generated by a control word generator 3 in a manner which is well-known. The control word is encrypted into an

Entitlement Control Message (ECM) by an ECM generator 4 using a service key SK, which is changed on, for example, a monthly basis. The ECM also includes access criteria which identify the service and the conditions required to access the service.

5   The service key is also encrypted by an encryption module 5 into another type of message, referred to as an Entitlement Management Message (EMM), using a fixed key FK which remains unchanged. EMM messages also carry details of the subscriber and his subscription.

The conventional form of ECM and EMM messages is defined in the

10   international standard ISO IEC 13818-1, the entire contents of which are incorporated herein by reference.

The encrypted broadcast stream together with the ECM and EMM messages is multiplexed in a multiplexer 6 with other broadcast streams representing other programmes, together making up a subscription package

15   from a particular service provider. The package is sent to a transmitter 7 from which it is transmitted, via a communications channel 8, for example a satellite or cable channel, using an appropriate modulation scheme. The encrypted broadcast stream is received at a subscriber's receiver 9, for example a satellite dish, and passed to the subscriber's decoder 10.

20   On receipt at the decoder, for example a set-top box (STB) 10, the received data is demultiplexed in a demultiplexer 11, to extract the required programme and its associated ECM and EMM messages. The extracted ECM and EMM messages are sent to a plug-in smart card 12. The smart card 12 uses the ECM and EMM messages to determine whether the subscriber has

25   the right to view the broadcast and if so, to decrypt the control word CW.

The smart card 12 includes the fixed key FK which is also present at the broadcasting side. This is used to decrypt the service key SK provided in the EMM messages. The decrypted service key SK is then used to decrypt the control word CW, which is input to a decryption module 13 together with the

30   scrambled broadcast stream to recover the original MPEG-II encoded broadcast stream. The encoded stream is passed to an MPEG-II decoder 14

which produces an output signal comprising audio, video and data components for display on the subscriber's television 15.

A recording device 16 located between the receiver 9 and the decoder 10 can be used to' record the encrypted signal as it is received, for subsequent
5   playback through the decoder 10.

The control word is changed at predetermined intervals, for example, every few seconds. A continuous stream of ECM messages is therefore required to decrypt the encrypted signal. The EMM message can be updated . less frequently, for example, the encrypted service key can be sent monthly.

10   Figure 2 illustrates a recording device according to the invention. This includes a demultiplexer 11, a smart card 12 and a decryption module 13 as in the conventional decoder 10 described above. The recording device further includes a processor 17, a second encryption module 18 and a storage medium 19, for example a hard disk or optical disk.

15   Referring to Figure 3, the incoming digital stream is split by the demultiplexer 11 and the smart card 12 into an encrypted video stream and a stream of control words (step s1). Each stream is fed to the decryption module 13, which uses the control word stream to decrypt the encrypted video signal (step s2), as in the conventional decoder 10 described above. The decrypted
20   video signal is then processed by the processor 17, with a view to manipulating it to make the signal easier to record or easier to play back (step s3). Examples of such manipulation include applying the conventional techniques of Packet Identification Number (PID) remapping, which refers to the transport packets in the MPEG-II scheme, as well as remultiplexing and
25   transcoding. In more detail, PID remapping comprises changing the audio and video PID of the incoming signal, which is chosen by the broadcaster, to a fixed number chosen by the recording device. Remultiplexing relates to altering Packetized Elementary Stream (PES) structures to be aligned with video frames and conversion from transport streams to program streams, while
30   transcoding relates to conversion of the MPEG-2 video to a lower bitrate MPEG-2 signal or conversion of the MPEG-2 video to another compression format such as H26L or MPEG-4.

After processing, the processed signal is re-encrypted at the second encryption module 18 using the control word stream from the smart card 12 (step s4). The second encryption module uses the same cryptographic algorithm, or cipher, as the first encryption module 2 at the broadcast side.

5   The encrypted video signal is then stored on the storage medium 19 (step s5).

When the video is played back from the storage medium 19, the decoder will receive an encrypted stream which uses exactly the same cipher and keys as the original broadcast. The decoder is therefore unable to detect that the video signal has been manipulated.

10   As mentioned above, the control word used for encryption changes frequently. The changes are synchronised with the incoming video stream and occur on a suitable boundary in the stream, for example at the start of a transport stream packet. Depending on the processing which is applied after decryption, it is likely that key changes in the encrypted video output will not

15   fall on convenient boundaries in the stream, since the processing will clearly take a finite time. If the decoder receiving the altered stream does not have its keys synchronised with the keys used by the re-encoding step, incorrect data will be produced in the receiver. To overcome this problem, a delay is introduced into the control word stream between the decryption module 11 and

20   the second encryption module 18, as shown in Figure 4 by the delay module 20. The delay module 20 adds a delay which allows a change in the control word being used to decrypt to be postponed until a suitable boundary occurs in the manipulated stream.

While embodiments of the invention have been described in relation to

25   a symmetric key system where the encryption and decryption keys are identical, variations on this are possible. For example, the encryption and decryption keys may be different but correspond to one another, where for example the decryption keys can be calculated from the encryption keys and vice versa. Similarly, the cryptographic algorithms used for encryption and

30   decryption need not be the same, but may be related functions. The only requirement is that a signal encrypted using the encryption algorithm and the encryption key can be recovered by applying the decryption algorithm and the

decryption key. As an alternative to using a symmetric algorithm, a different type of cryptographic system, including a public key based system, may be used.

From reading the present disclosure, other variations and modifications will be apparent to persons skilled in the art. Such variations and modifications may involve equivalent and other features which are already known in the field of digital transmission and cryptographic systems and which may be used instead of or in addition to features already described herein. Although claims have been formulated in this application to particular combinations of features, it should be understood that the scope of the disclosure of the present invention also includes any novel features or any novel combination of features disclosed herein either explicitly or implicitly or any generalisation thereof, whether or not it relates to the same invention as presently claimed in any claim and whether or not it mitigates any or all of the same technical problems as does the present invention. The applicants hereby give notice that new claims may be formulated to such features and/or combinations of such features during the prosecution of the present application or of any further application derived therefrom.

CLAIMS

1.   A method of storing a received digital signal which has been
encrypted by an encryption key and transmitted in encrypted form, comprising
5   the steps of:
         decrypting the signal using a decryption key corresponding to the
encryption key;
         processing the decrypted signal;
         re-encrypting the processed signal using the encryption key; and
10   storing the re-encrypted signal.

2.   A method according to claim 1, wherein the step of processing
the decrypted signal includes manipulating it to improve storage and/or
playback operation.
15

3.   A method according to claim 1 or 2, wherein the decryption key is
the same as the encryption key.

4.   A method according to any one of the preceding claims, wherein
20   the encryption key is one of a plurality of keys forming a key stream.

5.   A method according to claim 4, further comprising delaying the
key stream after decrypting the signal and before re-encrypting the processed
signal.
25

6.   A method according to claim 5, including delaying the key stream
in dependence on the processing being carried out on the decrypted signal.

7.   A method according to claim 5 or 6, wherein the digital signal
30   comprises a stream of transport packets, the method including synchronising
the key stream with the transport packet stream.

8.   A method according to any one of the preceding claims, wherein the step of processing the decrypted signal comprises performing the operations of Packet Identification Number (PID) remapping, remultiplexing or transcoding.

5

9.   A digital signal storage device for storing a digital signal which . has been encrypted using an encryption key and transmitted in encrypted form, the device comprising:

decryption means for decrypting the signal using a decryption key

10   corresponding to the encryption key;

means for processing the decrypted signal;

encryption means for re-encrypting the processed signal using the encryption key; and

means for storing the re-encrypted signal.

15

10.   A storage device according to claim 9, wherein the processing means comprises means for manipulating the decrypted signal to improve storage and/or playback operation.

20   11.   A storage device according to claim 10, wherein the processing means comprises means for performing the operations of Packet Identification Number (PID) remapping, remultiplexing and/or transcoding.

12.   A storage device according to any one of claims 9 to 11, wherein

25   the decryption key is the same as the encryption key.

13.   A storage device according to any one of claims 9 to 12, wherein the encryption key is one of a plurality of keys forming a key stream.

30   14.   A storage device according to claim 13, further including delay means for delaying the key stream prior to re-encrypting the decrypted signal.

15.   A storage device according to claim 14, wherein the delay means comprises means for synchronising the key stream with convenient boundaries within the signal.

5   16.   A storage device according to any one of claims 9 to 15, wherein the digital signal comprises a digital television signal.

17.   Digital signal recording apparatus for recording a digital signal which has been encrypted using an encryption key and transmitted in
10   encrypted form, the apparatus comprising:

a decryption module for decrypting the signal using a decryption key corresponding to the encryption key;

a processor for processing the decrypted signal;

an encryption module for re-encrypting the processed signal using the
15   encryption key; and

a storage medium for storing the re-encrypted signal.

18.   A method of storing a received digital signal substantially as hereinbefore described with reference to the accompanying drawings.
20

19.   A digital signal storage device substantially as hereinbefore described with reference to the accompanying drawings.

25

30

ABSTRACT

STORAGE OF ENCRYPTED DIGITAL SIGNALS

Digital video signals are encrypted by a broadcaster based on a key

5   stream and transmitted to a receiver.   At the receiver, the signals are
decrypted using the broadcaster's keys and processed in unencrypted form to
improve recording and/or playback operation. The processed signals are then
re-encrypted using the broadcaster's keys, with appropriate time-shifting to
align key changes with suitable boundaries in the video stream. The resulting

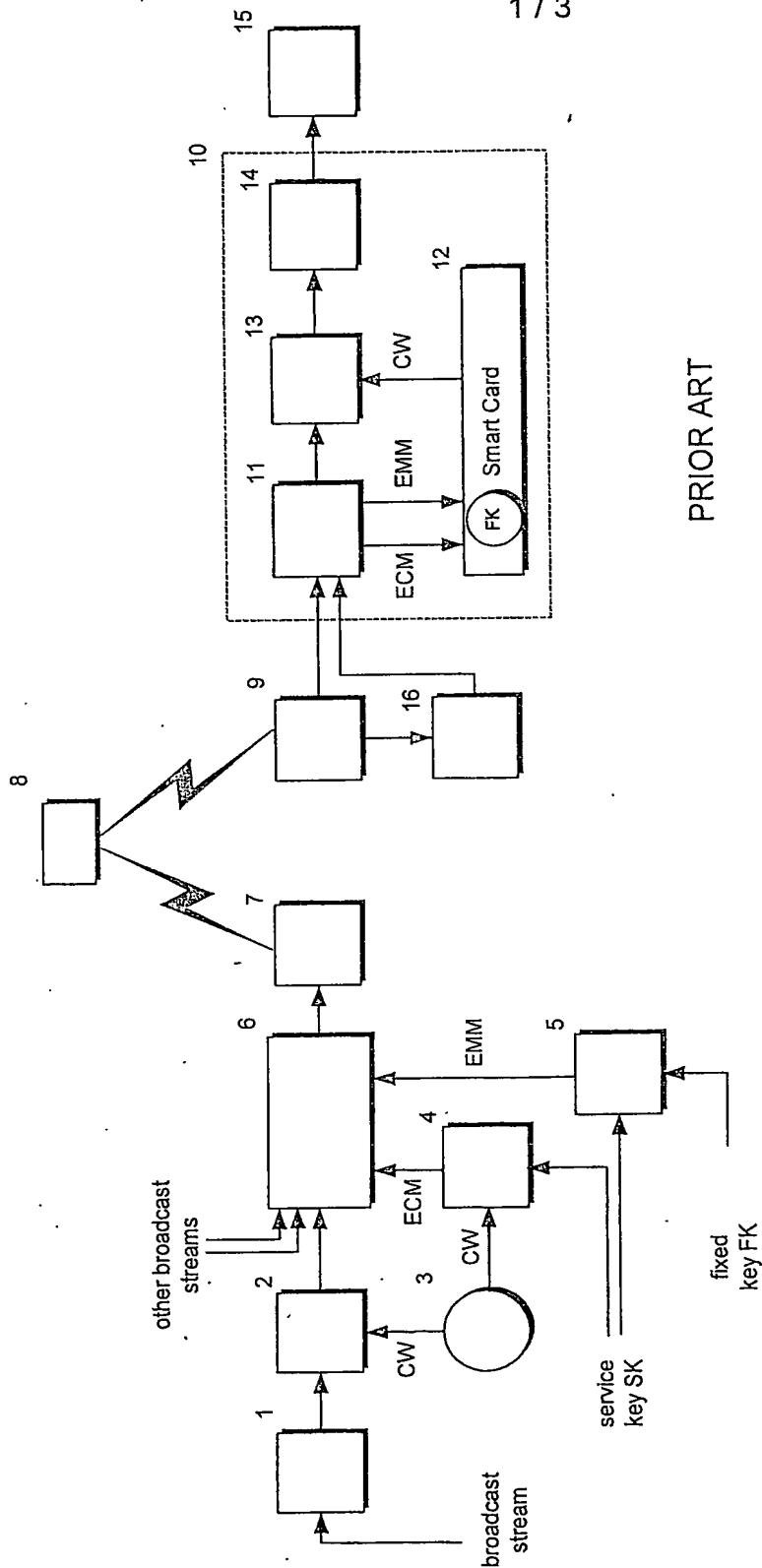10   encrypted signals are stored on a storage medium.
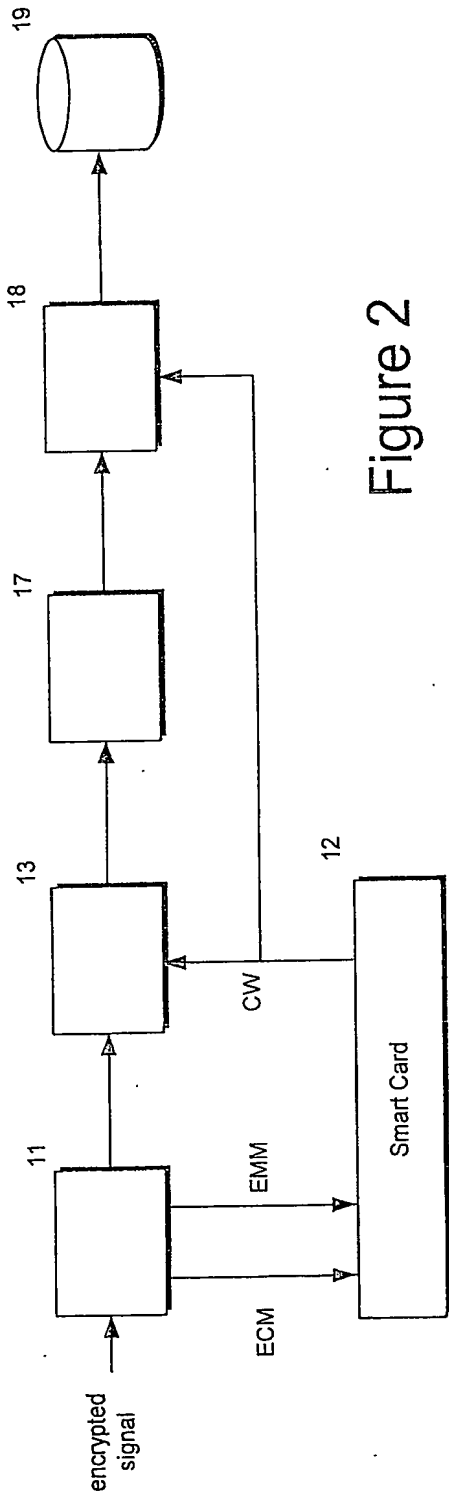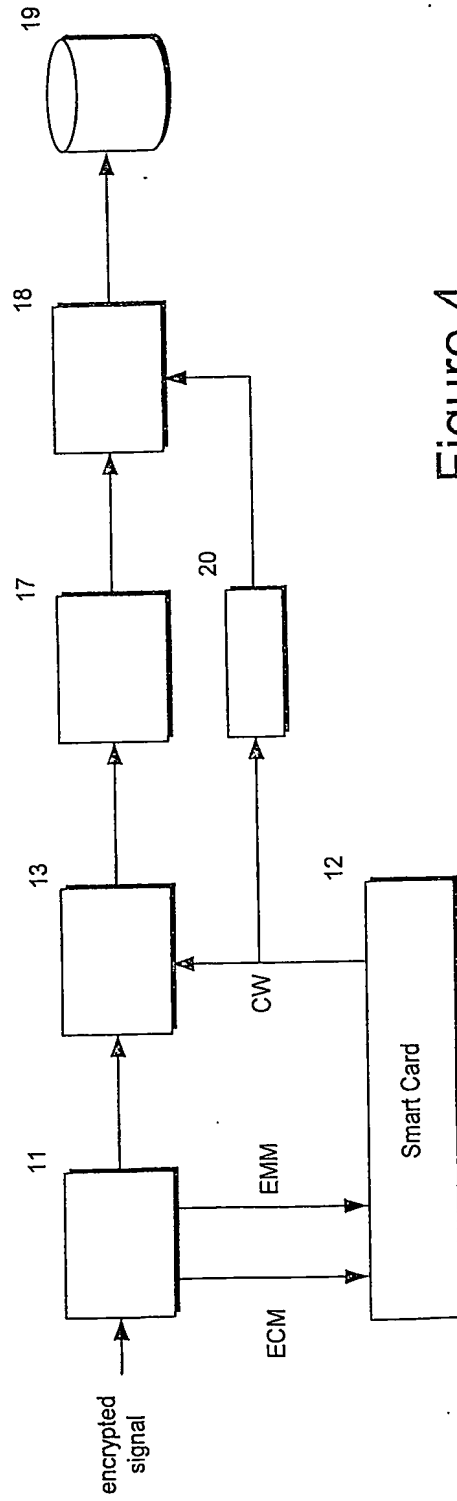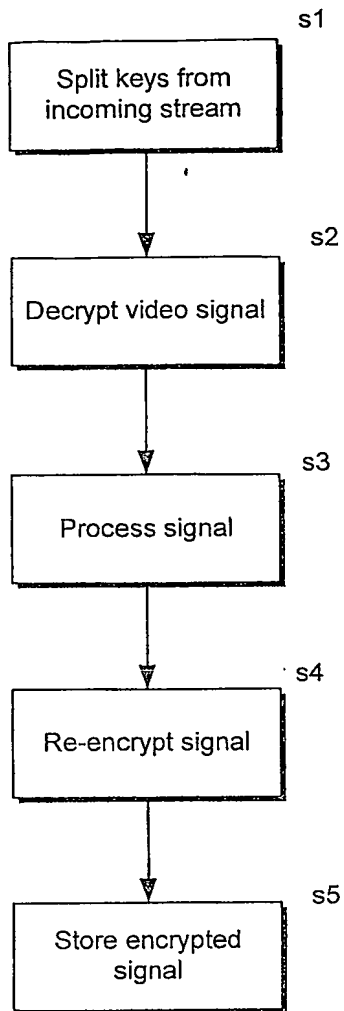
(Figure 4)

Figure 1

PRIOR ART

Figure 2

Figure 4

```
              ┌──────────────────────┐  s1
              │    Split keys from    │
              │   incoming stream     │
              └──────────────────────┘
                         │
                         ▼
              ┌──────────────────────┐  s2
              │   Decrypt video signal │
              └──────────────────────┘
                         │
                         ▼
              ┌──────────────────────┐  s3
              │     Process signal     │
              └──────────────────────┘
                         │
                         ▼
              ┌──────────────────────┐  s4
              │    Re-encrypt signal   │
              └──────────────────────┘
                         │
                         ▼
              ┌──────────────────────┐  s5
              │    Store encrypted     │
              │        signal          │
              └──────────────────────┘
```

Figure 3